



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/766,337	01/27/2004	Derek L. Davis	42P6514C	3287

7590 09/20/2007  
Blakely, Sokoloff, Taylor & Zafman LLP  
7th Floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025

EXAMINER
----------

FIELDS, COURTNEY D

ART UNIT	PAPER NUMBER
----------	--------------

2137

MAIL DATE	DELIVERY MODE
-----------	---------------

09/20/2007

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b> 10/766,337	<b>Applicant(s)</b> DAVIS DEREK L.	
	<b>Examiner</b> Courtney D. Fields	<b>Art Unit</b> 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 29 June 2007.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 2-11 and 13-19 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 2-11 and 13-19 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)                                | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                       | 5) <input type="checkbox"/> Notice of Informal Patent Application                       |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

**DETAILED ACTION**

1. Claims 1,12 and 20-21 have been cancelled.
2. Claims 2,13,15, and18 have been amended.
3. Claims 2-11 and 13-19 are pending.

***Response to Arguments***

4. Applicant's arguments with respect to claims 2-11 and 13-19 have been considered but are moot in view of the new ground(s) of rejection, Asano et al. (Pub No. 20020169971).

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 2-11 and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Asano et al. (Pub No. 20020169971) in view of Krawczyk, Hugo "New Hash Functions for Message Authentication".

As per claim 2, Asano et al. discloses a method for securing communications between a first device and a second device comprising:

mutually authenticating the first device (recording and reproducing device 300) and the second device (recording device 400) (See page 26, Sections 0392-393),

generating an integrity check vale by the first device (recording and reproducing device 300) (See page 26, Section 0399),

and sending the integrity check value with a message from the first device to the second device (See page 28, Section 0433)

However, Asano et al. does not explicitly disclose the feature of extracting bits from a pseudo-random data stream for use in a matrix having M rows and N columns. Krawczyk teaches a method and system which uses Toeplitz matrices.

Krawczyk discloses the claimed limitation of extracting bits randomly for use as coefficients of a matrix having M rows and N columns and performing operations to generate the integrity check value. (See pages 301-303)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 3, (Asano et al. as modified by Krawczyk) discloses the claimed limitation of inputting keying material into a cipher engine performing operations in accordance with a stream cipher and producing the pseudo-random stream by the cipher engine. (See Krawczyk, page 302)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system

Art Unit: 2137

by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 4, (Asano et al. as modified by Krawczyk) discloses the claimed limitation wherein a counter mode stream cipher in Data Encryption Standard. (See Krawczyk, page 304, Section 2.2, 1<sup>st</sup> and 2<sup>nd</sup> paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 5 and 9, (Asano et al. as modified by Krawczyk) discloses the claimed limitation of assigning M bits from the selected number of bits as a first column of the matrix and assigning M bits for each remaining column of the matrix. (See Krawczyk, page 307)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 6 and 10, (Asano et al. as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on M bits from the content of the message and coefficients of the first column of the matrix and performing an exclusive OR operation between each of the values to produce integrity check value. (See Krawczyk, page 304, Section 2.2, 1<sup>st</sup> paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 7, (Asano et al. as modified by Krawczyk) discloses the claimed limitation wherein the arithmetic operations are bitwise multiplication operations. (See Krawczyk, page 304, Theorem 3, and 3<sup>rd</sup> paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 8, (Asano et al. as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on the M bits from the message for a N-1 column of the matrix and performing exclusive OR operations between values associated with N-1 column of the matrix to produce N-1 bits of the integrity check value. (See Krawczyk, page 307, Section 3)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a

Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 11 and 17, (Asano et al. as modified by Krawczyk) discloses the claimed limitation of computing the integrity check value based on bits in the message, and determining if the bits differ from the predetermined bits set for the integrity check value. (See Krawczyk, page 309)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 13, (Asano et al. as modified by Krawczyk) discloses a method comprising:

decrypting an incoming message (See Asano et al., page 33, Section 0516),  
computing an integrity check value for an incoming message (See Asano et al., page 33, Section 0518)

and determining whether the incoming message is valid by comparing the computed integrity check value with the recovered integrity check value (See Asano et al., page 35, Section 0541)



Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claims 14, 15, and 16, (Asano et al. as modified by Krawczyk) discloses the claimed limitation of performing arithmetic operations on M bits from the content of the message and coefficients of the first column of the matrix and performing an exclusive OR operation between each of the values to produce integrity check value. (See Krawczyk, page 304, 1<sup>st</sup> and 2<sup>nd</sup> paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See Krawczyk, page 30 - Introduction)

As per claim 18, (Asano et al. as modified by Krawczyk) discloses the claimed limitation the first device includes a integrity check value generator to produce an integrity check value based on a selected group of its from a pseudo-random data stream and contents of the message. (See Krawczyk, page 308, Section 4 and page 309, 1<sup>st</sup> and 2<sup>nd</sup> paragraph)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See page 30 - Introduction)

As per claim 19, (Asano et al. as modified by Krawczyk) discloses the claimed limitation wherein the first device is a processor (See Asano et al., page 24, Section 0361) and the second device is a memory (See Asano et al., page 24, Section 0362)

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify Asano et al.'s data authentication system by combining Krawczyk's hash function for message authentication. This modification would have been obvious to a person having ordinary skill in the art because a person having ordinary skill in the art would have been motivated to extract bits from a pseudo-random data stream for use in a matrix having M rows and N columns by utilizing a

Art Unit: 2137

Toeplitz matrix as taught in Krawczyk in order to secure communication using matrix-vector multiplication. (See page 30 - Introduction)

**Conclusion**


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Courtney D. Fields whose telephone number is 571-272-3871. The examiner can normally be reached on Mon - Thurs. 6:00 - 4:00 pm; off every Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

  
cdf

September 15, 2007

  
MATTHEW SMITHERS  
PRIMARY EXAMINER  
*Art Unit 2137*